Notice of Allowability	Application No.	Applicant(s)	
	10/672,811	CHEUNG, TOM THUAN	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *24 September 2007*.

2. ☒ The allowed claim(s) is/are *1-6,9 and 13-20*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 1-6, 9 and 13-20 have been examined.

2. A Request for Continued Examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 24 September 2007 has been entered.

Response to Amendment

3. By this amendment, claims 1, 4-5, 13-15 and 18 have been amended. Claims 8, 10 and 12 have been cancelled. No new claims have been added.

Claim Objections

4. As a result of the amendment to the claims, the examiner withdraws the pending claim objection.

Claim Rejections - 35 USC § 112

5. As a result of the amendment to the claims, the examiner withdraws the pending claim rejection.

Claim Rejections - 35 USC § 101

6. As a result of amendment to the claims 15-17, the examiner withdraws the pending claim rejection.

7. The examiner withdraws the pending 101 rejections to the claims 18-20 due to the authorized examiner's amendment (Please see below examiner's amendment)

Response to Arguments

8. Applicant's argument filed 23 August 2007 have been fully considered and they are persuasive (See allowable subject matter below)

EXAMINER'S AMENDMENT

9. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Kelvin Vivian, on 11 October 2007.

Please amend the claims as follows:

(Claim 1) (Currently Amended) A computer-implemented method for encrypting and decrypting an original string that is storable in a database, the method comprising:

defining a set of factors to be used for encrypting the original string;

using an encryption equation to map the original string to an encrypted string, the encryption equation being a function of the original string and the set of factors;

using a set of derivative equations to ~~respectively~~ generate ~~a corresponding first~~ derivative values ~~value~~ from the set of factors;

storing the encrypted string and ~~each first~~ the generated derivative values ~~value~~ in the database;

providing one or more false derivatives that cannot be used to determine a given factor from the set of factors;

additionally storing ~~a~~ the one or more false derivative values ~~value~~ in the database with the generated derivative values~~, the false derivative value not being used to determine a given factor from the set of factors during decryption of the stored encrypted string~~;

using a set of factor decryption equations to map each of the ~~first~~ generated derivative values stored in the database to a corresponding factor in the set of factors; and

decrypting the encrypted string stored in the database using a decryption equation and each factor mapped through the set of factor decryption equations to generate a decrypted string that is equal to the original string.

wherein a presence of the one or more false derivative values with the generated derivative values in the database prevents an attacker from knowing which of the one or more false derivative values and the generated derivative values to use with the factor decryption equation to derive the factors in the set of factors.

(Claim 15) (Currently Amended) A system for encrypting and decrypting an original string, the system comprising:

a processor; and

a memory in communication with the processor, the memory storing a plurality of instructions that are executable by the processor, the plurality of instructions comprising instructions to implement,

an encryption module configured to:

receive user input defining a set of factors to be used for encrypting the original string;

receive user input defining an encryption equation that maps the original string to an encrypted string, the encryption equation being a function of the original string and the set of factors; ~~and~~

~~encryption~~

receive user input defining a set of derivative equations, ~~each~~ the set of derivative equations ~~equation~~ being used to generate a ~~corresponding first~~ derivative values ~~value~~ from the set of factors; and

provide one or more false derivatives that cannot be used to determine a given factor from the set of factors;

a database configured to store the encrypted string, ~~each first~~ the generated derivative ~~value~~ values, and a the one or more false derivative ~~value~~ values~~, wherein the false derivative value not being used to determine a given factor from the set of factors during decryption of the stored encrypted string~~; and

a decryption module configured to:

use ~~implementer~~ a set of factor decryption equations to map each of the ~~first~~ generated derivative values stored in the database to a corresponding factor in the set of factors; and

decrypt the encrypted string stored in the database using a decryption equation and each factor mapped through the set of factor decryption equations to generate a decrypted string that is equal to the original string,

wherein a presence of the one or more false derivative values with the generated derivative values in the database prevents an attacker from knowing which of the one or more false derivative values and the generated derivative values to use with the factor decryption equation to derive the factors in the set of factors.

(Claim 18) (Currently Amended) ~~A computer-readable medium encoded with a computer program for encrypting and decrypting an original string that is storable in a database, the computer program comprising computer executable code for:~~

A computer program stored in a computer readable medium to execute a method of encrypting and decrypting an original string that is storable in a database, said method comprising the steps of:

defining a set of factors to be used for encrypting the original string;

using an encryption equation to map the original string to an encrypted string, the encryption equation being a function of the original string and the set of factors;

using a set of derivative equations to ~~respectively~~ generate ~~a corresponding first~~ derivative values ~~value~~ from the set of factors;

storing the encrypted string and ~~each first~~ the generated derivative values ~~value~~ in the database;

providing one or more false derivatives that cannot be used to determine a given factor from the set of factors;

additionally storing ~~a~~ the one or more false derivative values ~~value~~ in the database with the generated derivative values~~, the false derivative value not being used to determine a given factor from the set of factors during decryption of the stored encrypted string~~;

using a set of factor decryption equations to map each of the ~~first~~ generated derivative values stored in the database to a corresponding factor in the set of factors; and

decrypting the encrypted string stored in the database using a decryption equation and each factor mapped through the set of factor decryption equations to generate a decrypted string that is equal to the original string,

wherein a presence of the one or more false derivative values with the generated derivative values in the database prevents an attacker from knowing which of the one or more false derivative values and the generated derivative values to use with the factor decryption equation to derive the factors in the set of factors.

(Claim 19) (Currently Amended) The computer program ~~product~~ of claim 18, wherein the set of factors comprises at least one of: constant values, numbers, objects, and random values that are derived from events.

(Claim 20) (Currently Amended) The computer program ~~product~~ of claim 18, wherein the set of factors comprises at least one of: constant values, numbers, objects, and random values that are derived from values provided by equations.

Allowable Subject Matter

10. Claims 1-6, 9 and 13-20 are allowed.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

11 October, 2007
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100